CLAIMS

What we claim is:

1. A method of manipulating data comprising converting $GF(2^{2s})$ representation data into corresponding $GF((2^s)^2)$ representation data by applying to said $GF(2^{2s})$ representation data a conversion operator related to a predetermined transformation.

2. The method of claim 1 wherein said conversion operator is related to a representation-transformation matrix corresponding to said transformation.

3. The method of claim 2 wherein said conversion operator comprises an inverse of said representation-transformation matrix.

4. The method of claim 2 wherein said conversion operator comprises a combination of a linear transformation and said representation-transformation matrix.

5. The method of claim 4 wherein said conversion operator comprises an inverse of a matrix product of said representation-transformation matrix and an AES S-box parameter matrix.

6. The method of any of claims 1-5 wherein said $GF((2^s)^2)$ representation is defined by an irreducible reduction polynomial over $GF(2^s)$ and an extension polynomial over $GF(2^s)$.

7. The method of claim 6 wherein said extension polynomial over $GF(2^s)$ comprises an irreducible polynomial of a second degree over $GF(2^s)$.

8. The method of any of claims 2-7 wherein said representation-transformation matrix is selected from a set of possible representation-transformation matrices based on a predetermined criterion.

9. The method of claim 8 wherein each matrix of said set of matrices is defined by a root of an irreducible polynomial over said $GF(2^{2s})$ representation, and a field generator of the $GF((2^s)^2)$ representation.

10. The method of any of claims 1-9 comprising processing said $GF((2^s)^2)$ representation data by performing at least one operation equivalent to at least one

desired operation in said $GF(2^{2s})$ representation to provide processed $GF((2^s)^2)$ data.

11. The method of any of claims 1-9 wherein said $GF(2^{2s})$ representation data comprises two or more data blocks, and wherein said method comprising processing said $GF((2^s)^2)$ representation data by performing on the two or more data blocks at least one operation in said $GF((2^s)^2)$ representation equivalent to at least one desired operation in said $GF(2^{2s})$ representation to provide processed $GF((2^s)^2)$ data.

12. The method of claim 10 or 11 comprising converting said processed $GF((2^s)^2)$ data back into said $GF(2^{2s})$ representation by applying to said processed $GF((2^s)^2)$ data a de-conversion operator related to said predetermined transformation.

13. The method of any of claims 1-12 wherein s equals four.

14. A secure memory storage device compliant with an AES S-box, comprising:

an input conversion module to convert $GF(2^{2s})$ representation data into corresponding $GF((2^s)^2)$ representation data;

an operations module to perform at least one operation equivalent to at least one desired operation in said $GF(2^{2s})$ representation to provide processed $GF((2^s)^2)$ data; and

an output conversion module to convert said processed $GF((2^s)^2)$ data back into said $GF(2^{2s})$ representation.

15. The device of claim 14 wherein said input conversion module comprises a multiplier to multiply a linear transformation of said $GF(2^{2s})$ data by a matrix related to a representation-transformation matrix.

16. The device of claim 14 or 15 wherein said at least one desired operation comprises an inverse operation.

17. The device of any of claim 14-16 wherein said output conversion module comprises a multiplier to multiply a linear transformation of said processed $GF((2^s)^2)$ data by a matrix related to a representation-transformation matrix.

18. The method of any of claims 14-17 wherein s equals four.

19.A method for determining a representation-transformation comprising:

synthesizing a plurality circuits corresponding to a plurality of representation-transformations from a $GF(2^{2s})$ representation into a $GF((2^s)^2)$ representation, respectively; and

selecting one of said plurality of representation-transformations based on at least one optimization criterion.

20.The method of claim 19 wherein synthesizing said plurality circuits comprises constructing said plurality of circuits.

21.The method of claim 19 or 20 wherein synthesizing said plurality circuits comprises simulating said plurality of circuits.

22.The method of any of claims 19-21 wherein s equals four.

23.The method of any of claims 19-22 wherein said plurality of representation matrices comprises 192 matrices.

24.The method of any of claims 19-23 wherein said at least one criterion comprises circuit area.

25.The method of any of claims 19-23 wherein said at least one criterion comprise power consumption.

26.A method for decrypting data comprising:

converting $GF(2^{2s})$ representation data into corresponding $GF((2^s)^2)$ representation data by applying to said $GF(2^{2s})$ representation data a decryption conversion operator related to a predetermined transformation;

processing said $GF((2^s)^2)$ representation data by performing at least one operation equivalent to a desired decryption operation in said $GF(2^{2s})$ representation to provide processed $GF((2^s)^2)$ data; and

converting said processed $GF((2^s)^2)$ data back into said $GF(2^{2s})$ representation.

27.A method for encrypting data comprising:

converting $GF(2^{2s})$ representation data into corresponding $GF((2^s)^2)$ representation data by applying to said $GF(2^{2s})$ representation data a predetermined transformation;

processing said $GF((2^s)^2)$ representation data by performing at least one operation equivalent to a desired encryption operation in said $GF(2^{2s})$ representation to provide processed $GF((2^s)^2)$ data; and

converting said processed $GF((2^s)^2)$ data back into said $GF(2^{2s})$ representation by applying to said processed $GF((2^s)^2)$ data an encryption conversion operator related to said predetermined transformation.

28.The method of any of claims 1-13 wherein applying said conversion operator comprises applying one or more intermediate conversion operators to recursively convert said $GF(2^{2s})$ representation data into said $GF((2^s)^2)$ representation data.

29.An encryption/decryption device comprising:

an input conversion module to convert data in a $GF(2^{2s})$ representation into corresponding data in a $GF((2^s)^2)$ representation, said input conversion module comprising decryption conversion circuitry and encryption conversion circuitry;

an operations module to perform at least one operation equivalent to a desired encryption/decryption operation in said $GF(2^{2s})$ representation to provide processed $GF((2^s)^2)$ data; and

an output de-conversion module to convert said processed $GF((2^s)^2)$ data back into said $GF(2^{2s})$ representation, said output conversion module comprises decryption de-conversion circuitry and encryption de-conversion circuitry.